

Application no.: 09/592,165
Amdt date: April 30, 2004
Reply to Office Action of January 30, 2004

Amendments to the Specification:

✓ Please amend the paragraph starting on page 1, line 5 as follows:

A¹
This application claims the benefit of U.S. provisional applications 60/138,849, 60/138,850, 60/139,033, 60/139,034, 60/139,035, 60/139,036, 60/139,038, 60/139,042, 60/139,043, 60/139,044, 60/139,047, 60/139,048, 60/139,049, 60/139,052, 60/139,053, all filed June 10, 1999, and U.S. provisional application 60/139,076, filed on June 11, 1999, the contents of all of which are incorporated herein by reference. This application also contains subject matter that is related to the subject matter disclosed in U.S. Patent Application Nos. 09/592,442, 09/592,443, 09/591,802, 09/591,801, 09/592,163, 09/592,079, and 09/592,083, all filed on June 12, 2000.

✓ Please amend the paragraph starting on page 9, line 26 as follows:

A²
As illustrated in FIG. 2, each object in the structure is preferably stored as an LDAP entry. At the top of the hierarchy is the policy server domain object 201 including various policy server resources and a plurality of policy domains objects (generally referenced at [[204]] 240). Each policy domain object 240 is a grouping of policy enforcers that share common policies. Each policy domain object 240 includes a resource root object 200 and a group root object 202. All policy management functions are preferably implemented in terms of the resource objects which include devices 204, users 206, hosts 208, services 210, and time 220. Thus, a firewall policy may be defined by simply assigning the particular devices, users, hosts, services, and time applicable to the policy. The devices, users, hosts, and services are preferably organized in groups 212, 214, 216, and 218, respectively, having a group name, description, and member information for a more intuitive way of addressing and organizing the resources.

✓ Please amend the paragraph starting on page 17, line 8 as follows:

A³
FIG. 7 is a screen illustration of an exemplary global monitor user interface 402 presenting various types of health and status information. Such information may relate to

Application no.: 09/592,165
Amdt date: April 30, 2004
Reply to Office Action of January 30, 2004

A3
the health of the device, such as system load 712 and network usage information 714.

The information may also relate to current alarms 716 on the device including alarm name, type, description, and the like. The information may further relate to current VPN connections [[718]] 717 including connection type, source/destination, duration, and VPN traffic volume.

[✓] Please amend the paragraph starting on page 36, line 23 as follows:

A4
In addition to the above, each log entry includes an in-bytes field [[832]] 834 indicative of the number of bytes the policy enforcer received as a result of the activity, and an out-bytes field [[834]] 836 indicative of the number of bytes transferred from the policy enforcer. Furthermore, a duration field [[836]] 838 indicates the duration (e.g. in seconds) of the activity.

[✓] Please amend the paragraph starting on page 42, line 9 as follows:

A5
In step 436, the policy server 122 checks whether the updates have been successful. In this regard, the policy server 122 waits to receive an acknowledgment from the policy enforcer that the updates have been successfully completed. Upon a positive response from the policy enforcer, the policy server 122 deletes the apply attribute 270e for the policy enforcer's log DN 270e in step 438. Otherwise, if the update was not successful (e.g. because the policy enforcer was down), the apply log is re-sent the next time another apply function is invoked. Alternatively, the failed policy enforcer transmits a request to the policy server 122 of the log of non-applied changes when it rejoins the network (e.g. by rebooting).

[✓] Please amend the paragraph starting on page 47, line 11 as follows:

A6
FIG. 30 is an exemplary flow diagram of updating the primary and backup units when the primary unit is nonfunctional. In step 978, the primary unit becomes nonfunctional, and in step 980, the network administrator sends/transmits an upgrade directly to the backup

52

A

Application no.: 09/592,165
Amdt date: April 30, 2004
Reply to Office Action of January 30, 2004

*Ab
trial.*

unit instead of the primary unit. In step 982, the backup unit updates itself with the information received from the management station and waits for the primary unit to become functional. Once the primary unit becomes functional in step 984, the update is automatically sent/transmitted to the primary unit for upgrading in step 986. The primary unit then updates itself in step 988.
